

PATENT

Atty Docket No.: D03045
App. Ser. No.: 10/712,427

IN THE CLAIMS:

Please find below a listing of all of the pending claims. The statuses of the claims are set forth in parentheses.

1. (Original) A method of encoding a common data stream for distribution to a plurality of destination systems, each destination system being authorized to access at least a portion of the common data stream, the method comprising:

obtaining a source stream;

identifying a first set of blocks of said source stream as secure blocks;

identifying a second set of blocks of said source stream as unsecure blocks;

encrypting said secure blocks for each of a plurality of classes of destination systems, thereby forming a plurality of encrypted secured block sets, such that an encrypted secured block set is decryptable by destination systems in a class associated with that encrypted secured block set; and

grouping said unsecured blocks and the plurality of encrypted secured block sets as the common data stream.

2. (Original) The method of claim 1, wherein said source stream is packetized video data.

3. (Original) The method of claim 1, further comprising encrypting unsecure blocks such that said unsecure blocks are decryptable by each of said plurality of destination systems, if authorized by at least one conditional access system.

PATENT

Atty Docket No.: D03045
App. Ser. No.: 10/712,427

4. (Original) The method of claim 1, wherein encrypting comprises encryption utilizing at least one of AES, with at least one AES key per class of destination systems, and DES, with at least one DES key per class of destination systems.

5. (Original) The method of claim 1, wherein said blocks are MPEG blocks and said secure blocks represent MPEG I frames.

6. (Currently Amended) A method of decoding a common data stream distributed to a plurality of destination systems, wherein said common data stream includes secure and unsecure blocks of data, said secure blocks being encrypted for each of a plurality of classes of destination systems, respectively, said method comprising:

obtaining said common data stream;

decrypting said secure blocks for [[a]] each native class of [[a]] each of the destination systems, thereby forming decrypted secure block sets for the plurality of classess of the destination systems; and

grouping said unsecure blocks and said decrypted secure block sets as a useful stream for use by said destination system.

7. (Original) The method of claim 6 further comprising demultiplexing said common data stream into said secure and said unsecure blocks.

PATENT

Atty Docket No.: D03045
App. Ser. No.: 10/712,427

8. (Original) The method of claim 6, wherein decrypting comprises decryption utilizing at least one of AES, with at least one AES key per class of destination systems, , and DES, with at least one DES key per class of destination systems.
9. (Original) The method of claim 6 further comprising providing a decryption key for said step of decrypting.
10. (Original) The method of claim 6 further comprising discarding secure blocks of any non-native class.
11. (Original) The method of claim 6, wherein said blocks are MPEG blocks and said secure blocks represent MPEG I frames.
12. (Original) An encoder system for encoding a common data stream for distribution to a plurality of destination systems, each destination system being authorized to access at least a portion of the common data stream, said encoder system comprising:
 - an input for receiving a source stream;
 - an encoder, said encoder receiving said source stream and packetizing said source stream to provide a plurality of packets; and
 - an encryptor for selectively identifying at least one set of blocks of said packets as secure blocks and encrypting said secure blocks for each of a plurality of classes of destination systems, thereby forming a plurality of encrypted secured block sets, such that an

PATENT

Atty Docket No.: D03045
App. Ser. No.: 10/712,427

encrypted secured block set is decryptable by destination systems in a class associated with that encrypted secured block set.

13. (Original) The encoder system of claim 12, wherein said encryptor combines said encrypted secure blocks and said unsecure blocks to form a common data stream.

14. (Original) The encoder system of claim 12, wherein said encoder is an MPEG encoder.

15. (Original) The encoder system of claim 12, wherein said encryptor is at least one of a DES encryptor and an AES encryptor.

16. (Original) An encoder system for encoding a common data stream for distribution to a plurality of destination systems, each destination system being authorized to access at least a portion of the common data stream, said encoder system comprising:

an input for receiving a source stream;

an encoder, said encoder receiving said source stream and packetizing said source stream to provide a plurality of packets;

encryption selector for selectively identifying at least one set of blocks of said packets as secure blocks; and

an encryptor for encrypting said secure blocks for each of a plurality of classes of destination systems, thereby forming a plurality of encrypted secured block sets, such that an encrypted secured block set is decryptable by destination systems in a class associated with that encrypted secured block set.

PATENT

Atty Docket No.: D03045
App. Ser. No.: 10/712,427

17. (Original) The encoder system of claim 16, wherein said encryptor combines said encrypted secure blocks and said unsecure blocks to form a common data stream.
18. (Original) The encoder system of claim 16, wherein said encoder is an MPEG encoder.
19. (Original) The encoder system of claim 16, wherein said encryptor is at least one of a DES encryptor and an AES encryptor.
- 20-23. (Canceled).
24. (Original) A content transport system, comprising:
- a selector for selecting blocks to be encrypted as secured blocks;
 - a secure block multi-encryptor, for encrypting said secured blocks for each of a plurality of classes of destination systems, thereby forming a plurality of encrypted secured block sets, such that an encrypted secured block set is decryptable by destination systems in the class associated with that encrypted secure block set;
 - a combiner for combining unsecure blocks and secure blocks into a common stream;
 - a demultiplexer for separating said common stream into blocks that are usable by a destination system and blocks that are not usable by the destination system;
 - a selective decryptor that decrypts usable secured blocks; and

PATENT

Atty Docket No.: D03045
App. Ser. No.: 10/712,427

a reassembler for reassembling a useful signal stream from any unsecure blocks, and said secure blocks decrypted by the selective decryptor, wherein an ability to reassemble the useful signal stream relies in part on an ability to decrypt usable secure blocks.

25. (Original) The system of claim 24, wherein the reassembler is an MPEG decoder.

26. (Currently Amended) A computer-readable ~~carrier~~ medium that is a physical memory storage device, the computer-readable medium including a common data stream comprising:

a plurality of secure blocks encoded from a source stream, said plurality of secure blocks encrypted for each of a plurality of classes of destination systems, thereby forming a plurality of encrypted secured block sets, such that an encrypted secured block set is decryptable by destination systems in a class associated with that encrypted secured block set; and

a plurality of unsecured blocks encoded from said source stream.

27. (Currently Amended) A computer-readable ~~carrier~~ medium that is a physical memory storage device, the computer-readable medium including computer program instructions for distribution to a plurality of destination systems, each destination system being authorized to access at least a portion of the common data stream that instruct a computer to perform the steps of:

obtaining a source stream;

identifying a first set of blocks of said source stream as secure blocks;

PATENT

Atty Docket No.: D03045
App. Ser. No.: 10/712,427

identifying a second set of blocks of said source stream as unsecure blocks;

encrypting said secure blocks for each of a plurality of classes of destination systems, thereby forming a plurality of encrypted secured block sets, such that an encrypted secured block set is decryptable by destination systems in a class associated with that encrypted secured block set; and

grouping said unsecured blocks and the plurality of encrypted secured block sets as the common data stream.

28. (Currently Amended) A computer-readable ~~carrier~~ medium that is a physical memory storage device, the computer-readable medium including computer program instructions for decoding a common data stream distributed to a plurality of destination systems, wherein said common data stream includes secure and unsecure blocks of data, said secure blocks being encrypted for each of a plurality of classes of destination systems, respectively, that instruct a computer to perform the steps of:

obtaining said common data stream;

decrypting said secure blocks for ~~[[a]]~~ each native class of ~~[[a]]~~ each of the destination systems, thereby forming decrypted secure block sets for the plurality of classess of the destination systems; and

grouping said unsecure blocks and said decrypted secure block sets as a useful stream for use by said destination system.